FINAL @2012-05-21 – RIEŠENIA

1 (True or False) and Justify [20 bodov]

Uveďte, či je tvrdenie pravdivé a nanajvýš tromi vetami svoj názor zdôvodnite.

(Úplne správna odpoveď je za 2.5 boda. Správna odpoveď úplne bez zdôvodnenia je za 0.5 boda. Nesprávna odpoveď, ako aj správna odpoveď s úplne nesprávnym zdôvodnením, sú za 0 bodov.)

Q1 Ak je f čiastočne rekurzívna funkcia, tak jej definičný obor a jej obor hodnôt sú rekurzívne vyčísliteľné množiny.

Q2 Nech f je nejaká unárna čiastočná funkcia na množine $\mathbb{N}$. Jediné, čo o f vieme, je, že jej definičný obor je rekurzívna množina. Potom existuje rekurzívne zúplnenie f.

Q3 Pre každú rekurzívnu množinu X (vrátane okrajových prípadov!) platí $X \leq_m \{1, 2, 3\}$.

Q4 Nech f je unárna primitívne rekurzívna funkcia. Nech g je unárna rekurzívna funkcia, ktorá nie je primitívne rekurzívna. Potom $\exists n_0 : \forall n > n_0 : g(n) > f(n) + 47$.

Q5 Nech $A, B \subseteq \mathbb{N}$. Ak existuje **prostá** rekurzívna funkcia f taká, že $\forall n \in \mathbb{N} : a \in A \iff f(a) \in B$ a $B = \{f(a) \mid a \in A\}$, tak $A \equiv_m B$.

Q6 Nech $A, B \subseteq \mathbb{N}$. Ak $A \equiv_m B$, tak existuje **prostá** rekurzívna funkcia f taká, že $\forall n \in \mathbb{N} : a \in A \iff f(a) \in B$ a $B = \{f(a) \mid a \in A\}$.

Q7 Existuje funkcia f, ktorá je bijekciou na $\mathbb{N}$, je rekurzívna, ale nie je primitívne rekurzívna.

Q8 Množina dokázateľných tvrdení v Zermelo-Fraenkelovej axiomatizácii teórie množín je rekurzívne vyčísliteľná.

2 (True or False) and Justify – riešenie [20 bodov]

Q1 TRUE. Pre obor hodnôt ľahko spravíme generátor „paralelnou“ simuláciou f na všetkých vstupoch. Pre definičný obor tak isto, len keď nájdeme výpočet, ktorý skončil, nepridáme do vygenerovanej množiny hodnotu, ktorú vypočítal, ale vstup, z ktorého začínal.

Q2 FALSE. Samotná f môže byť natoľko zložitá, že tú časť vstupov, na ktorej je definovaná, nevieme algoritmicky počítať. Konkrétnym kontrapríkladom je napr. Busy beaver (aj $\mathbb{N}$ je rekurzívnou podmnožinou $\mathbb{N}$). Iná možnosť je zvoliť si konkrétnu nekonečnú rekurzívnu podmnožinu $\mathbb{N}$ a argumentovať tým, že jej zodpovedajúcich funkcií f je nespočítateľne veľa.

Q3 TRUE. Ako redukcia vždy zafunguje napr. funkcia „if $x \in X$, return 1, else return 0“. (Pre $X = \emptyset$ a $X = \mathbb{N}$ neplatí opačná „nerovnosť“.)

Q4 FALSE. Napr. f ľubovoľná a g definovaná pomocou unárnej Ackermannovej funkcie a nasledovne: $\forall n : g(2n) = a(n)$ a $\forall n : g(2n + 1) = 0$.

Q5 Za upozornenie na chybu ďakujem Peťovi Kostolányimu. Toto bolo zamýšľané riešenie:

TRUE. Táto f je priamo many-one redukciou A na B.

A všetko by bolo OK, keby som do zadania napísal $A \leq_m B$, ako som myslel. Lenže som napísal $A \equiv_m B$ a to už platiť nemusí. Celé to zakape samozrejme na tom, že nemusí existovať opačná redukcia. (Napr. v prípade $A = \mathbb{N}$ a $f(n) = n + 1$.)

Správna odpoveď je teda FALSE. Aby sme boli tolerantní, riešenia s rovnakou chybou ako moje dostanú 2 body.

Q6 FALSE. Napr. $\{1\} \equiv_m \{1, 2\}$, ale keďže tieto množiny majú rôzne mohutnosti, neexistuje f spĺňajúca uvedené požiadavky. (Každá f zjavne určuje bijekciu medzi A a B.)

Q7 TRUE. Opäť zoberme unárnu Ackermannovu funkciu a. Definujme $X = \{a(n) \mid n \in \mathbb{N}\}$ a nech x_i je i-ty najmenší prvok komplementu X (indexované od 0). Definujme funkciu g nasledovne: $\forall n : g(2n) = a(n)$ a $\forall n : g(2n+1) = x_n$. Takto definovaná funkcia je zjavne bijektívna. A tiež sa ľahko presvedčíme, že je rekurzívna – na výpočet $g(2n)$ stačí vedieť počítať $a(n)$, na výpočet $g(2n+1)$ stačí vypočítať hodnoty $a(0)$ až $a(n)$ a potom ísť v cykle od 0 a nájsť n-tú (indexované od 0), ktorá medzi nimi nie je.

Q8 TRUE. Toto vieme povedať aj bez toho, aby sme si presne pamätali, ako táto teória vyzerá. Rekurzívna vyčísliteľnosť množiny dokázateľných tvrdení je logickým dôsledkom mechanickej overiteľnosti platnosti dôkazu.

3 Známa pôda [12 bodov]

V tejto aj v nasledujúcej úlohe sa pýtam na priamo odprednášané veci, ukážte, že im dostatočne rozumiete.

a) (3 body) Definujte, čo je to vypočítateľné reálne číslo. (Za 3 body je moderná definícia.)
b) (9 bodov) Definujte konkrétne reálne číslo, ktoré nie je vypočítateľné.

4 Známa pôda – riešenie [12 bodov]

V podúlohe a) sa dali dostať 2 body za korektné definície typu „pre každé n viem vygenerovať n-tú cifru za desatinnou čiarkou“, resp. 3 body za lepšie definície typu „pre každé n viem dané číslo aproximovať zlomkom, pričom spravím chybu nanajvýš $1/n$“. V podúlohe b) sa buď dalo definovať Chaitinovu konštantu, alebo zobrať ľubovoľnú nie rekurzívnu množinu a definovať to číslo pomocou jej charakteristickej funkcie. Napr. $h = \sum_{n \in HALT} 2^{-n}$.

5 Známa pôda 2 [11 bodov]

Dokážte, že každá trieda ekvivalencie relácie $\equiv_m$ (ekvivalencia množín vzhľadom na many-one redukciu) je nanajvýš spočítateľne veľká.

6 Známa pôda 2 – riešenie [11 bodov]

Toto bola ťažšia úloha, lebo si v nej treba rozmyslieť správny smer úvah (pre opačný to nefunguje). Správna argumentácia vyzerá nasledovne: Majme ľubovoľnú množinu A. Uvažujme všetky množiny B_i také, že $B_i \leq_m A$. Pre každú B_i teda existuje nejaká redukcia f_i z B_i na A. Žiadne dve spomedzi redukcii B_i nemôžu byť rovnaké, lebo ak b patrí do symetrického rozdielu B_i a B_j, tak sa f_i a f_j musia líšiť na vstupe b. No a všetkých programov je len spočítateľne veľa, a tým skôr je spočítateľne veľa všetkých programov, ktoré fungujú ako redukcie z rôznych B_i na A.

(Opačným smerom je problém v tom, že na dôkaz $A \leq_m C_1$ aj $A \leq_m C_2$ môže fungovať tá istá redukcia.)

Vieme teda, že pre ľubovoľnú A existuje len spočítateľne veľa množín, ktoré sú od A „menšie alebo rovné“, a teda nutne existuje len spočítateľne veľa takých, ktoré sú s A ekvivalentné.

7 Exkurzia do neznáma [15 bodov]

V tejto úlohe sa pýtam na niečo, čo som neprednášal, a chcem vidieť, ako si s tým poradíte.

Uvažujme Minského registrové stroje s presne 4 registrami, ktoré počítajú unárnu čiastočnú funkciu (v registri 0 stroj dostane vstup, a ak výpočet skončí, v registri 1 máme výstup). Takéto stroje budeme volať *tetry*. Rôzne tetry sa od seba líšia tým, koľko a akých inštrukcií tvorí ich program. Počet inštrukcií v programe budeme volať *veľkosť tetry*.

Budeme sa pozerať len na to, čo tieto stroje robia, keď dostanú na vstupe nulu. Pre konkrétny stroj máme v princípe tri možnosti: buď jeho výpočet neskončí, alebo bude výsledkom výpočtu nula, alebo ním bude nejaká kladná hodnota. Stroje, pre ktoré výpočet skončí a jeho výsledkom je 0, budeme volať *zachovávajúce nulu*.

Definujme teraz funkciu ζ (zeta) nasledovne: $\zeta(n)$ je počet tetier veľkosti n zachovávajúcich nulu. Dokážte alebo vyvráťte každé z nasledujúcich tvrdení:

a) (10 bodov) Funkcia ζ je rekurzívna.
b) (2 body) Funkcia ζ je čiastočne rekurzívna, ale nie je rekurzívna.
c) (3 body) Funkcia ζ rastie rýchlejšie ako hocijaká rekurzívna funkcia.

8 Exkurzia do neznáma – riešenie [15 bodov]

V podúlohe a) dokážeme, že funkcia ζ nie je rekurzívna. Tento dôkaz si necháme na koniec. Podúloha b) následne zjavne neplatí: ζ je totálna, zatiaľ čo funkcie, ktoré sú čiastočne rekurzívne ale nie rekurzívne, totálne nie sú.

Ani podúloha c) neplatí. V tetre veľkosti n môžeme mať tak zhruba (podľa presnej definície inštrukčnej sady) $8 + 4(n + 1)$ rôznych inštrukcii – 4 pre zvýšenie registra, 4 pre zníženie, 4 možnosti, ktorý otestovať na 0 a $n + 1$ možností, kam potom skočiť. Takže celkový počet tetier v závislosti od ich veľkosti udáva funkcia $c(n) = (4n + 12)^n$. Toto je rekurzívna funkcia a ζ zjavne nemôže od nej rásť rýchlejšie.

A teraz už sľubovaný dôkaz, že ζ nie je rekurzívna. Sporom. Nech je. Ukážeme, že potom je rekurzívna aj množina $HALT$, čo bude hľadaný spor. Ako rozhodnúť, či $n \in HALT$? Vyrobme tetru, ktorá (bez ohľadu na vstup, a teda aj na vstupe 0) simuluje funkciu f_n na vstupe n, a ak zastane, vráti 0. Táto tetra má nejaký počet stavov x. Vypočítame $z = \zeta(x)$. A teraz paralelne simulujeme všetky tetry veľkosti x na vstupe 0, až kým buď naša tetra neskončí, alebo nenájdeme z iných tetier, ktoré skončia a vrátia 0.